



# Michigan CSI prevodilački projekt

Brošure priložene:

*Osnove cyber-zlostavljanja  
Michigan CSI internet izvori  
Ugovor o internet sigurnosti  
Pitanja za diskusiju o socijalnoj mreži & Plan akcije  
Upozoravajući signali/10 uputa za internet sigurnost*

Jezični prijevodi:

**Španski**  
**Arapski**  
**Mongolški**  
**Kineski**  
**Bosanski**  
**Albanski**  
**Rumunski**

**KONTAKT:**

Jenifer Esch, Menadžer programa  
Michigan CSI  
Department of Attorney General  
6<sup>th</sup> Floor G Mennen Williams Building  
525 West Ottawa Street  
Lansing, MI 48911  
Telefon: 517-335-0855  
E-mail adresa: [eschjl@michigan.gov](mailto:eschjl@michigan.gov)  
Web stranica: [www.michigan.gov/csi](http://www.michigan.gov/csi)



# Michigan CSI

(Michigan Pokretač cyber sigurnosti i)



## Osnove o zlostavljanju preko interneta

Zlostavljanje, koje se odvijalo na način ispisivanja na zidovima unutar WC-ova sada, kada je 99 procenata tinejdžera povezano tehnološkim aparatima je napredovalo sa napretkom tehnologije.

Cyber-zlostavljanje koristi internet ili mobilni telefon za prijetnju, ogovaranj/eširenje trača ili oglašavanje imidža. Mnogi tinejdžeri su zlostavljeni kada netko ukrade njihovu lozinku (password) ili druge osobne informacije te pošalje štetne poruke sa njihove e-mail adresе, osobne web stranice ili stranice za socijalno druženje. Sposobnost interneta da dospije u širu publiku u roku od nekoliko sekundi pravi ga perfektnim mjestom za prijatelje, neprijatelje ili druge osobe bez lica za zlostavljanjem drugih tinejdžera.

Cyber-zlostavljanje može zvučati zabavnim u početku, ali može imati ozbiljne dugoročne posljedice. Sve što se stavi na internet ostavlja digitalni otisak koji se može pratiti i gledati od strane drugih, uključujući i buduće kolege ili poslodavce. Vrlo je važno da se imati na umu slijedeće činjenice kada se služi internetom:

- **Internet je vječan:** Šta god se postavi na internet može se ponovo pronaći čak i kada je to izbrisano.
- **Niste anonimni:** Internet je javni forum. Sve se može pogledati i otkriti od strane Vašeg ISP-a.
- **Budite svjesni da uvijek ne znate s kime razgovarate.**
- **Promislite prije nego nešto postavite na internet:** Osigurajte zaštitu svoga imena, identiteta i reputacije.

Većina zlostavljanja započne u maloj mjeri, nalikujući na privatno podbadanje između prijatelja, a onda se proširi poput gljive u javni forum sve dok u potpunosti ne izađe iz kontrole podbadača. Svako je potencijalna meta. Polovina učenika priznaje da su bili zlostavljeni preko interneta, dok otprilike 79 procenata tinejdžera kaže da to predstavlja problem. Postoje vrste zaštite protiv cyber-zlostavljanja:

- **Nikada ne odgovoriti na vatru ili internetsko zlostavljanje.** Zlostavljač obično traže od drugih vatrenu reakciju a onda to pretvore u daljnje zlostavljanje.
- **Uvijek blokirati zlostavljača od slanja dalnjih poruka.** Programi zaštite (Spyware programi) su napravljeni tako da šalju zlostavljuće poruke u nastojanju da im njihova meta odgovori.
- **Odabrati podešenja (setting) tako da omogućuju pregled svih komentara i oglasa drugog korisnika prije nego postanu javnima.**
- **“Drugari ili prijatelji” trebaju biti obrisani ukoliko oni postave ikakav komentar ili imidž kojemu je svrha sramoćenje, prijetnja ili zlostavljanje..**
- **Dokumentovati i prijaviti zlostavljanje.** Reći povjerljivoj odrasloj osobi i prijaviti na ISP ili Web servis kao što su to MySpace ili AIM. Vrlo je važno pozvati policiju ako vam se prijeti ili prijaviti cyber-zlostavljanje internetom na [cybertipline.com](http://cybertipline.com).



## Michigan CSI internet izvori



Obrazovne aktivnosti za djecu – igre/slagalice/itd.



Informaciono za roditelje/nastavno osoblje



Sadržava video ili crtice



Zaštitini alat kompjutera



Informacije o cyber-zlostavljanju

**Disney Surf Swell – Internet sigurnost** – <http://disney.go.com/surfswell/>

Djeca putuju sa Mikijem i prijateljima i prikupljaju dragulje dok uče o razmjeni osobnih informacija, virusa i internet naljapnicama.

**iKeepSafe ili Internet Keep Safe Coalition** – [www.ikeepsafe.org](http://www.ikeepsafe.org)

Kuća Faux Paw i Techno mačke (The home of Faux Paw – the Techno Cat), knjiga i crtici koji uče predškolce do uzrasta 3-eg razreda o sigurnosti na internetu. Stranica sadržava video snimke za roditelje i djecu, knjige i stranice za bojanje.

**i-SAFE** – [www.isafe.org](http://www.isafe.org)

Programi za nastavno osoblje, roditelje, bake i djedove, te učenike. Registracija obavezna. Pogledati video snimke da bi se postalo "certifikovanim" i kvalifikovanim za besplatne materijale. Odličan nastavni materijal o sigurnosti na internetu, mjesecne novine i različiti tekstovi o sigurnosti na internetu.

**ISP ( Internet pružaoc usluga - Internet Service Provider) alatke:**

**AOL roditeljska kontrola** – <http://daol.aol.com/safetycenter/parentalcontrols>

Opcije za sveukupnu roditeljsku kontrolu.

**AT&T/Yahoo roditeljske kontrole** – [http://help.yahoo.com/sbc/tutorials/ypc/start\\_pc1.html](http://help.yahoo.com/sbc/tutorials/ypc/start_pc1.html)

Dio besplatnog AT&T Yahoo! Soba internet zaštite, uključujući i kontrole web filtera, rukovanje e-mailovima, IM kontrole, izvještaje.

**Comcast roditeljske kontrole** - <http://www.comcast.net/security/>

Roditeljske kontrole prate i logiraju se gdje djeca borave na internetu, uključujući i praćenje chat sesije, uzrastu-odgovarajuće stepene pristupa i aktivnosti logiranja na internetu.

**Media Awareness Network** – [www.media-awareness.ca](http://www.media-awareness.ca)

Kanadska web stranica sa odličnim izvorima informacija uključujući i online flesh igrice za uzrast 8-12 godina koje se odnose na privatnost i opasnost od chat soba. Ova stranica ima svaobuhvatan pristup obrazovanju o internetu.

**Naomi** – [www.radiance.m6.net](http://www.radiance.m6.net) i K9 Web Protection [www.k9webprotection.com](http://www.k9webprotection.com)

Dva besplatno programa internet filtera. Naomi je organizovan u Italiji; K9 u U.S.A.

## **Net Safe of New Zealand** – [www.netsafe.org.nz](http://www.netsafe.org.nz)



Skinite "Hector Protector," dugme sa delfinom u kutu vašeg kompjuterskog ekrana. Ako je dijete nečim uplašeno, kliktanje na Hector-a postavlja podvodnu scenu na ekranu i potrudnu poruku da zatraži pomoć odrasle osobe.

## **Net Smartz** – [www.netsmartz.org](http://www.netsmartz.org)



Istinite životne pričice, video streamovi, karte sa aktivnostima i brošure. Videote snimke o cyber-zlostavljanju i uzrastu odgovarajući crtici koji uči i sigurnosti na internetu. Aktivnosti dizajnirane za sve uzraste služe kao dobra početne točke za diskusiju o sigurnosti interneta za djecu svih uzrasta.

## **MySpace savjeti:**

### **Uklanjanje lažnog/uvredljivog računa (False/Offensive Account) u sličnosti osoblja /Staff's Likeness**

Ako član školskog osoblja otkrije da je lažni ili uvredljivi MySpace račun kreiran sa njihovom sličnošću i/ili identitetom, MySpace će ukloniti profil u pitanju. Pošaljite email na [schoolcare@myspace.com](mailto:schoolcare@myspace.com) sa školskog emaila i uključite slijedeće:

1. Web adresu lažnog i/ili uvredljivog profila, koji možete kopirati i zalijepiti na glavni dio (body) vašeg emaila sa web preglednika.
2. Kratko objašnjenje u kojem ćete dati dovoljno informacija kako biste pokazali da je profil lažan ili uvredljiv; te
3. Vaše ime i titulu, te ime, adresu i broj telefona škole gdje ste zaposleni.

### **Prijavljivanje računa maloljetnog učenika (<14)**

Ako školsko osoblje otkrije učenika ispod 14 godina koji ima svoj MySpace račun, osoblje može poslati email adresu maloljetnog učenika na [schoolcare@myspace.com](mailto:schoolcare@myspace.com) tako da MySpace može ukloniti taj račun. Pošaljite email sa školske email adrese i uključite slijedeće:

1. Web adresu učenikovog profila;
2. Vaš odnos sa učenikom;
3. Stvarna uzrast učenika i kako ste s time upoznali; te
4. Vaše ime i adresu, te ime, adresu i broj telefona škole gdje radite i koju učenik pohađa.

### **Instrukcije za uklanjanje MySpace računa**

Na vašoj stranici ([www.myspace.com](http://www.myspace.com)) spustite se do dna i odaberite "Savjeti za sigurnost/Safety Tips." Odaberite tipku "Savjeti za roditelje i nastavno osoblje/Tips for Parents and Educators". Spustite se do dna sve dok ne vidite naslov "Uputstva za uklanjanje MySpace računa/Instruction for Deleting a MySpace Account." Trebat ćete se logirati kako korisnik za što je potrebna email adresa vašeg djeteta i lozinka. Ukoliko ne znate lozinku vašeg djeteta, možete je zatražiti tako što ćete kliknuti na "Zaboravio lozinku/Forgot Password?" link u kućici za logiranje na MySpace.com. Lozinka će vam biti poslata na email adresu koja se koristi za logiranje na MySpace.

## **PRIJAVITE INTERNET PREDATORE**

**Michigan Department of Attorney General  
Child and Public Protection Unit  
1-888-KIDS-CSI  
1-888-543-7274  
[www.michigan.gov/ag](http://www.michigan.gov/ag)**

## **PRUŽITE POV RATNU VEZU ILI PODNESITE PITANJA NA MICHIGAN CSI**

**Michigan Department of Attorney General  
Michigan CSI  
1-877-765-8388  
[AGCSI@michigan.gov](mailto:AGCSI@michigan.gov)**



# Michigan CSI

(Michigan Pokretač cyber sigurnosti i)



## Ugovor o internet sigurnosti

- 1) Neću davati nikakve osobne informacije online bez saglasnosti povjerljive odrasle osobe. Ovo uključuje moje ime, broj telefona, adresu, e-mail adresu, lokaciju moje škole, adresu/broj telefona mojih roditelja na poslu, kredit kartice te moju sliku. Ovo vrijedi za sve na internetu, uključujući email adresu, sobe za chat, web stranice koje mi obećavaju besplatne stvari i nagrade, te za materijal koji ja postavim na internet.
- 2) Kada se služim internetom, ja ću se uvijek služiti pretendiranim imenom ili nadimkom koji ne otkriva moje ime, uzrast, te da li sam dječak ili djevojčica.
- 3) Kada kreiram lozinku/ password, napravit ću je takvu da ju je teško pogoditi, ali za mene je laka za sjetiti se. Da bi se izbjegla krađa lozinke nikada je nikom neću reći (osim mojim roditeljima) – čak ni svojim najboljim prijateljima.
- 4) Neću odgovarati na bilo koje poruke koje me prave neprijazan osjećaj. Pokazat ću ih odrasloj osobi odmah.
- 5) Nikada se neću sastati sa osobom s kojom sam se povezao/la putem interneta.
- 6) Nikada neću slati uvredljivu ili okrutnu poruku bilo kome online.
- 7) Nikada neću onesposobiti bilo koji filter ili posmatrački softver na kompjuteru zato što je tu postavljen da bih ja bio/la siguran.
- 8) Neću otvarati e-mailove, datoteke/filove, linkove, slike ili igrice od ljudi koje ne poznam ili im ne vjerujem. Uvijek ću prvo upitati odraslu osobu.
- 9) Neću uzimati riječi, slike ili zvukove sa nečije web stranice bez njihove saglasnosti.
- 10) Neću vjerovati u sve što pročitam na internetu. Uvijek ću provjeriti izvor informacije i potvrditi ga sa svojim nastavnikom, roditeljem ili bibliotekarom.
- 11) Jedino ću se služiti internetom u ove dane/vremena \_\_\_\_\_.
- 12) Dozvoljeno mi je da se služim internetom na \_\_\_\_\_ minuta; tada ću raditi nešto drugo.

Potpisano: \_\_\_\_\_  
Dijete – Ja ću se držati ovih pravila.

Datum: \_\_\_\_\_

Potpisano: \_\_\_\_\_  
Odrasla osoba – ja neću **pretjerano reagovati** kada mi dijete kaže o nekim lošim stvarima koje su se desile u cyber prostoru. Ja ću smireno raditi sa svojim djetetom, kako bi osigurao sigurno internet iskustvo.

Datum: \_\_\_\_\_



# Socijalno druženje

## Pitanja za diskusiju & Plan akcije

**Pitanja za diskusiju.** Razgovarajte sa svojim djetetom o informacijama u profilu; te zajedno pregledajte profil koji je on ili ona kreirala. Ohrabrite Vaše dijete da dijele svoje internet iskustvo. Evo nekih pitanja samo za početak:

1. Za što si koristio internet?
2. Da li imaš e-mail adresu? Koliko? Koje su? Koje su lozinke?
3. Da li imaš profil? Koliko? Gdje su ti profili? Koja su ti korisnička imena i lozinke?
4. Šta misliš koliko su privatne tvoje informacije koje si postavio na internet? Ko to može vidjeti?
5. Da li misliš da to službenici na prijemu za fakultet mogu vidjeti? Šta o mogućim poslodavcima?
6. Da li te je ikad neko nepoznat kontaktirao preko interneta? Kako si odgovorio?
7. Da li se neko ikad poslužio internetom da to kaže nešto što te vrijeđa? Šta se desilo?
8. Da li si video seksualne imidže ili primjedbe na tvojoj stranici ili profilu? Šta si uradio kao odgovor na to?

**Plan akcije.** Ako otkrijete da Vaše dijete ima profil na stranici socijalne mreže, razmotrite slijedeći plan:

1. Dajte svom djetetu dan da "očisti/clean-up" njegov ili njen profil te zajedno provjerite novi profil(e).
2. Čuvajte trenutne bilješke o informacijama o korisničkim imenima Vašeg djeteta, uključujući sve e-mail adrese, korisnička imena, prikazana imena i lozinke.
3. Redovno provjeravajte mrežu prijatelja Vašeg djeteta na svakoj web stranici. Ako ima imena ljudi koje ne poznate, upitajte svoje dijete ko su i kako su ih upoznali. Uklonite "jedino online prijatelje/online only friends" sa profila Vašeg djeteta. Pogledajte profile prijatelja da vidite šta oni otkrivaju o Vašem djetetu.
4. Učestalo provjeravajte sadržaj na profilu Vašeg djeteta. Da li Vaše dijete postavlja neodgovarajuće osobne informacije, slike, video snimke, blogove ili komentare? Da li se Vaše dijete uključuje u zlostavljanje ili drugo neodgovarajuće ponašanje? Ako jeste, uklonite sadržaj.
5. Provjerite podešenja računa na profila Vašeg djeteta. Na primjer, možete modifikovati "Podešenja računa /Account Settings" na profilu MySpace.com da biste ga napravili "privatnim," ili da provjerite korisnike koje je Vaše dijete blokiralo.

# **Upozoravajući znakovi**

1. Vaše dijete provodi veliki dio vremena on-lina, pogotovo uveče.
2. Pronašli ste pornografiju na kompjuteru Vašeg djeteta.
3. Vaše dijete je imalo telefonske pozive od ljudi koje ne poznajete ili bira brojeve telefona, ponekad i van lokalne linije, koji su Vam nepoznati.
4. Vaše dijete je primilo poštu, poklone ili pakete od nekog koga ne poznajete.
5. Vaše dijete brzo gasi monitor ili brzo mijenja sliku na ekranu svaki put kada se pojavit u sobu.
6. Vaše dijete se povlači od ostatka porodice.
7. Vaše dijete koristi online račun koji pripada nekom drugom.
8. Kada je online, Vaše dijete koristi mikrofon ili web kameru za koju niste znali da ga on/ona ima.

## **10 savjeta za sigurnost interneta**

1. Napravite jasna i jednostavna pravila za djecu kojih će se pridržavati.
2. Postavite kompjuter sa pristupom internetu na lokaciju na kojoj je vidljiv ostalim članovima porodice (ne u djetetovoj sobi).
3. Objasnite svojoj djeci da nikada ne smiju davati prepoznatljive informacije – ime, kućnu adresu, ime škole ili broj telefona – u javnim forumima kao što su to to chat sobe ili oglasna ploča (novine) ili ljudima koje ne poznaju.
4. Diskutujte o važnosti toga da Vama ili povjerljivoj odrasloj osobi kaže ukoliko Vaše dijete ili tinejdžera ikada išta uplaši, stvori neugodnost ili ga zbumuje dok je online.
5. Upoznajte se sa Internetom i svim sevisima koje Vaše dijete koristi.
6. Upoznajte se sa blokiranjem i programima praćenja.
7. Nikad ne dozvolite djetetu da ugovori lice-u-lice sastanak sa drugim korisnikom, bez roditeljske saglasnosti ili društva.
8. Recite svojoj djeci da nikada ne odgovaraju na poruke ili predmete sa oglasne ploče koje su sugestivne, nepristojne, ratoborne, prijeteće ili im izazivaju neprijatan ugodaj.
9. Prijavite poruke koje predstavljaju opasnost lokalnim organima zakona.
10. Podsetite svoju djecu da ljudi online možda nisu (a vjerovatno nisu) onakvi kakvima se predstavljaju; te da sve što ljudi kažu online možda i nije istina.



*The translation of these documents was partially funded by Wayne RESA, NCLB Title III.*